

(19)

Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 0 955 761 A1

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:

10.11.1999 Bulletin 1999/45

(51) Int Cl. 6: H04L 29/12

(21) Application number: 99400380.4

(22) Date of filing: 17.02.1999

(84) Designated Contracting States:

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE

Designated Extension States:

AL LT LV MK RO SI

(30) Priority: 03.03.1998 US 33870

(71) Applicant: SUN MICROSYSTEMS, INC.
Palo Alto, California 94303 (US)

(72) Inventors:

- Martin, Jean-Christophe
Route de Beauregard, 38760 Varces (FR)
- Duloutre, Sylvain
38600 Fontaine (FR)

(74) Representative: Harris, Ian Richard et al

D. Young & Co.,
21 New Fetter Lane
London EC4A 1DA (GB)

(54) Network directory access mechanism

(57) A computer-implemented directory access mechanism provides a directory service operable to access a network directory under a predetermined protocol by responding to an access request under the protocol for information available in a predetermined environment external to the directory. The directory service then uses the access method for the environment to access the information available in the environment. In this manner, data in the given environment can be accessed

by a directory service operable under the given protocol by configuring an attribute access method and using this method to retrieve the information. The protocol can be the Lightweight Directory Access Protocol. The information to be accessed could typically be an attribute of an entry in the directory. An access control list (for example the Directory Access Control Domain) can contain not only control access rights for directory objects, but also the access methods for attributes of the directory objects.

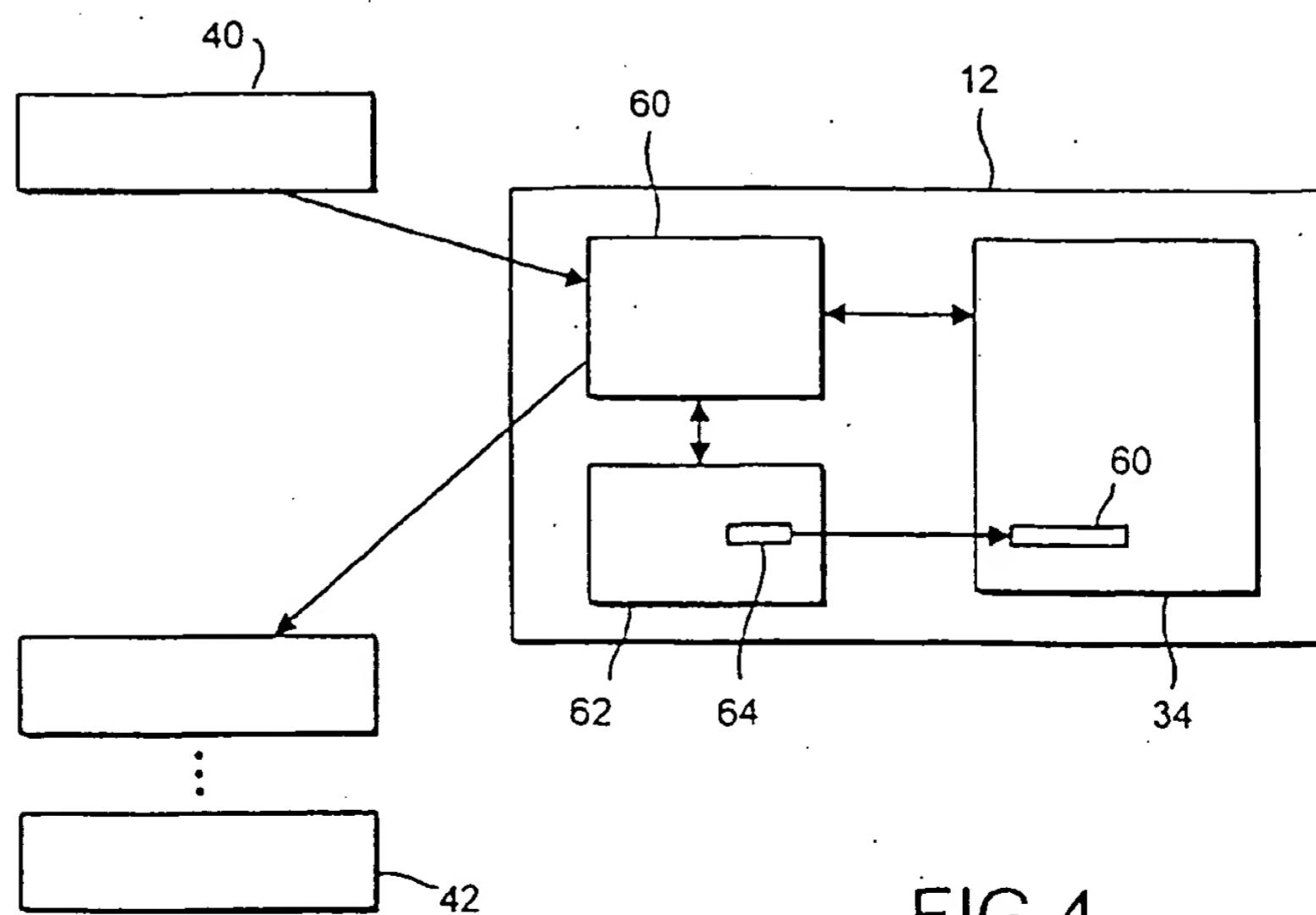


FIG.4.

EP 0 955 761 A1

Description**BACKGROUND OF THE INVENTION**

5 [0001] This invention relates to a network directory access mechanism, for example access mechanisms based on Directory Access Control Domains (DACDs) on the Internet.

[0002] The popularity of directory servers based on ISO/CCITT X.500 model has increased with the wide support by the industry of the Lightweight Directory Access Protocol (LDAP). LDAP is defined by RFC 1777. There is a desire to try to integrate heterogeneous information in these directories by either moving the data from their old format to this 10 new model, or to map the old model into the X.500 model. However, this is not straightforward and has practical difficulties.

15 [0003] The directory services under the X.500 model are based on an object hierarchy, with each node in the hierarchy corresponding to a given level of detail. A particular location in the hierarchy is identified by the sequence of nodes down the hierarchy from the root or base node to the node in question. Each entry in the hierarchy sets out attributes for the entry. Although there is a single logical hierarchy, parts of the hierarchy can be physically separated. In order for the practical hierarchy to operate, therefore, each node identifies the physical location of the adjacent nodes down the hierarchy.

20 [0004] To access the hierarchy, access control lists are provided. These can be provided at nodes throughout the hierarchy and define access control rights for different users and/or bodies. The access control rights relate to areas of the local structure (domains) of the hierarchy and not to the physical locations of the nodes of the attributes for the hierarchy. Thus, if it is intended to provide access under the LDAP, for example, to information created under a pre-existing, non-X.500 format, it is necessary to copy the whole of the previous directory to the new directory accessed through LDAP.

25 [0005] The present invention seeks to provide a solution to the problem of how to integrate into a directory service operable under a first format directory entries under a second format, without needing to convert all of the entries under the first format into the second format.

SUMMARY OF THE INVENTION

30 [0006] Particular and preferred aspects of the invention are set out in the accompanying independent and dependent claims. Combinations of features from the dependent claims may be combined with features of the independent claims as appropriate and not merely as explicitly set out in the claims.

[0007] In accordance with a first aspect of the invention, there is provided a computer-implemented directory access mechanism. The method comprises steps of:

35 i) a directory service operable to access a network directory under a predetermined protocol responding to an access request under the protocol for information available in a predetermined environment external to the directory; and

ii) the directory service using an access method for the environment to access the information.

40 [0008] Thus, an embodiment of the invention enables a directory service operable under a predetermined directory access protocol to access data in a predetermined environment (e.g. data stored in accordance with a different storage model from that on which the predetermined protocol is based, or a different physical location, or a different protocol) by configuring an attribute access method and using this method to retrieve the information from, for example, a directory operable in the predetermined environment.

45 [0009] In a preferred embodiment of the invention the access method configuration is achieved by extending a domain definition normally used for access control. Where reference is made to an access method, this forms an access process or procedure, typically implemented by a set of access parameters or computer instructions or a combination thereof. Preferably, the access method is retrieved via a domain definition for a domain of the directory. The domain definition can also include access control information. In a preferred embodiment of the invention, the directory is defined under X.500 and the access method is retrieved from a Directory Access Control Domain object.

50 [0010] However, the invention is not limited to associating the access method with access control. Thus it is possible for an access method to be defined without access control, on a specific attribute.

[0011] The domain definition can include a pointer to an access method for the domain in the environment, possibly stored externally to the directory or possibly stored with a definition of a node in the directory.

55 [0012] In the preferred embodiment of the invention, the protocol is the Lightweight Directory Access Protocol. The information to be accessed could typically be an attribute of an entry in the directory.

[0013] Thus, a preferred embodiment of the invention uses the Directory Access Control Domain (Dacd) as defined

in the ISO/CCITT X.501(1993 E) specification not only to store access rights but also to store access methods. The access method points to a directory entry storing the specific access method parameters.

[0014] In accordance with another aspect of the invention, there is provided a directory access mechanism comprising a directory service to access a network directory operable under a predetermined protocol, at least one identifier of an access method for access to information in a predetermined environment external to the directory, the directory service being configured to respond to an access request under the protocol to access the information in said environment using an access method identifier.

[0015] In accordance with a further aspect of the invention, there is provided a directory access mechanism comprising a directory service configured to be operable to access to a network directory under a predetermined protocol and to identify at least one access method for access to information in a predetermined environment external to the directory, the directory service being configured to respond to an access request under the protocol to access the information available in the environment using an access method identifier.

[0016] In accordance with yet a further aspect of the invention, there is provided an Access Control List (ACL) for a network directory service, which access control list comprises control access rights for directory objects and access methods for attributes of the directory objects. The access control list can form a computer implemented access control mechanism for an object-based directory.

[0017] The invention also provides a computer program product on a carrier medium, the computer program product comprising a directory service configured to be operable to provide directory access under a predetermined protocol, and at least one identifier of an access method for information in a predetermined environment external to the directory, the directory service being configured to respond to an access request under the protocol to access the information available in the environment using an access method identifier.

[0018] The invention further provides a directory server for a computer network, the directory server comprising storage for a network services directory under a predetermined protocol and at least one identifier of an access method for information in a predetermined environment external to the directory, and a processor for executing a directory service controller, the directory service being configured to respond to an access request under the predetermined protocol to access the information available in the environment using an access method identifier.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] Exemplary embodiments of the present invention will be described hereinafter, by way of example only, with reference to the accompanying drawings in which like reference signs relate to like elements and in which:

Figure 1 is a schematic representation of a directory structure for a network directory service;
 Figure 2 is a schematic representation of a telecommunications environment including a plurality of stations interconnected via a network;
 Figure 3 is a schematic representation of a client server station;
 Figure 4 is a schematic representation of a directory server;
 Figure 5 is a schematic representation of a message format for a directory access protocol; and
 Figure 6 is a flow diagram of the operation of a directory controller.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0020] Figure 1 is a schematic representation of a conventional directory information structure arranged as an object hierarchy. The directory information structure enables information on network users and resources to be stored.

[0021] The directory structure comprises, for example, a tree-shaped hierarchy 2 of nodes 3, 4 etc leading from a root node 3 to a plurality of entries 5 forming the leaves of the hierarchy. Within the hierarchy, there are defined domains, for example domain A 5 and domain B 6.

[0022] Associated with a domain, there is defined an Access Control List (ACL). The ACLs define access control rights for different users and/or bodies. The ACL for a given domain is associated with the highest node within the domain and defines the access control rights for the domain. The ACL has the required granularity, but not the semantic of the access method. For example, it could not be possible to define that entries such as telephone numbers are stored in one database and entries e-mail addresses are stored in another database. As a result, integration of non-X.500 based attribute data is not possible according to the conventional model without copying all of the original information into the entries concerned. For example, if e-mail addresses for the entries 5 in domain A were stored in a different database, it would be necessary to make a complete copy of that information into the database for the entries 5.

[0023] Figure 2 of the accompanying drawings is a schematic representation of an instance of a computer network where a five stations 10, 12, 14, 16 and 18 communicate via a network 20. The network could be a local area network (LAN), wide area network (WAN), or an intra- or Inter-network. Each of the stations could be formed by a single computer

5 or by a network of computers, for example a LAN or WAN. Also, although only five stations are shown, it will be appreciated that a typical computer network includes many more stations arranged in a complex interconnection structure. The interconnection structure could be at one logical level, or could employ at least in part a hierarchical structure. The individual stations can make variable demands on the system, both relative to each other and over time. In a typical situation, a relatively smaller number of the stations will form server stations and a relatively larger number of the stations will form client stations. In Figure 2, stations 10 and 18 are assumed to support a directory service master 14 and a directory service slave 20, respectively and that stations 12, 14 and 16 support appliances including a Directory User Agent (DUA) 28.

10 [0024] Particular embodiments of the invention will now be described which are based on the LDAP protocol in the context of an Internet application. However, it will be appreciated that the invention is not limited thereto, and that the invention finds application to any communications network application where it is desired to integrate directories operable under different protocols.

15 [0025] In a specific embodiment of the invention, the Directory Access Control Domain (DACD) as defined in the ISO/CCITT X.501(1993 E) specification is used, not only to store access rights but also to store access methods. The access method can point to a directory entry storing specific database access method parameters, whereby it is possible to leave the non-X.500 data in its original location, and still be able to access the information using LDAP.

20 [0026] Figure 3 is a schematic block representation of an embodiment of the invention. In Figure 3, a directory service 32 includes a directory database 34 located on a server 30. The database 34 contains an X.500 directory database.

25 [0027] A Directory User Agent (DUA) 38 for an appliance 36 forms a directory user client for accessing the directory service 32 to read information from or to write information to the directory 34. It will be appreciated that there will typically be a large number of appliances and DUAs 38 requiring and making access to the directory service 32. Only one appliance 36 and DUA 38 are shown in Figure 3, however, for illustrative purposes and ease of explanation.

30 [0028] Access by the DUA 38 to the directory service 32 is by way of request 40 and response 42 messages under a conventional protocol, here LDAP. Thus, the client 38 will solicit one or more response messages 42 by issuing a request 40 to the directory service 32. The request message 40 may be a request for information about, for example, an attribute of a network user or a network resource (for example an Internet protocol (IP) address for the user or resource). The server 30 will then return one or more response messages 42 to the request 40. The request and response messages will be linked to each other by the use of related message identifiers in the messages, typically in headers for the messages.

35 [0029] Also shown in Figure 3 is a further database 48, on a further server 44. The further database 48 may form part of another directory service operable under another protocol, or may simply be a database containing information relevant to the database on the directory server 30 but in a non-compatible format. In the present example it is assumed that the further database 48 is a switch database for a public switched telephone network switch 46. The switch database 48 contains telephone number information, at least some of which numbers relate to entries in the directory database 34.

40 [0030] In an embodiment of the invention, the directory service 32 at the server 30 comprises a DACD mechanism which defines not only access rights for domains but also access methods. The DACD mechanism can be constructed in accordance with ISO/CCITT X.501 (1993 E) except that it stores not only information relating to access control rights (i.e. who can access what) but also information about access control methods (i.e. how to access what). In a preferred form of the invention, the access control methods in the DACD mechanism comprises pointers to directory entries containing specific database access parameters. In this manner, integration of non-X.500 database attributes is possible without having to copy all of the database attributes to an X.500 format.

45 [0031] Figure 4 is a schematic representation of aspects of a directory service master 32 of an embodiment of the invention relevant to an understanding of the invention. The directory service includes the directory service database 34 and a directory controller 60. The directory controller 60 is responsive to a request message 40 from a DUA 38 to perform the operations necessary with respect to the database 16 and to return one or more response messages 42 to the user.

50 [0032] Figure 5 contains a schematic representation of an LDAP message format (LDAP message) 50 which provides an envelope containing common fields required in all protocol exchanges. The LDAP message provides a sequence with a message identifier (message ID) 52 followed by a protocol operator (protocol OP) 54. The message ID has a unique value compared to that of all other outstanding requests in an LDAP session. The message ID is echoed in all responses corresponding to a request in which the message ID was initially used.

55 [0033] The protocol operation specified by an LDAP message can conventionally be selected from the following types:

bindRequest	- initiates a protocol session between a client and a server and sets out the parameters for the session;
-------------	---

(continued)

5	bindResponse unbindRequest searchRequest	- returns an indication of the status of the client's request for initiation of a session; - terminates a session and has no response defined; - enables a client to initiate a search and defines: the base object in the directory with respect to which the search is to be performed; the scope of the search to be performed; an indication of how aliases are to be handled; a maximum search result size to be returned; a time limit for the search; indication of which attributes are to be returned and whether attribute types and/or values are to be returned; and a filter defining match characteristics;
10	searchResponse	- returns the response to a search request, wherein a sequence of responses will typically be necessary in order to return the full response to the request from the client;
15	modifyRequest modifyResponse addRequest addResponse delRequest delResponse	- enables a client to request modification of an object in the directory; - returns the result of the modification request; - enables a client to request addition of an object to the directory; - returns the result of the addition request; - enables a client to request deletion of an object to the directory;
20	modifyRDNRRequest modifyRDNRResponse compareDNRequest compareDNResponse abandonRequest	- returns the result of the deletion request; - enables a client to request modification of the last component (Relative Distinguished Name) of the name of an entry in the directory; - returns the result of the RDN modification request; - enables a client to compare an attribute value with an entry in the directory; - returns the result of the comparison request; - enables abandonment of a request.
25		

[0034] Thus the directory controller 60 is arranged to perform the operations necessary to be able to return the appropriate responses to the different requests identified above.

[0035] In responding to an access request, the directory controller 60 is responsive to a DACD 62 to identify a pointer 64 to a directory entry 66 containing database access control parameters for a database in the requested attributes are stored.

[0036] Thus, it is possible, for example, to specify that telephone numbers attributes are to be retrieved from the telecom switch equipment at the switch 46 directly through the access method appropriate for the switch (e.g., by direct access to the switch database 46, or by use of a proprietary protocol) without any copy of the telephone number needing to be kept in the directory 34. Thus, when a read request for the telephone number of an entry in the database 34 is received by the directory server 32 under LDAP, the telephone number attributes are not read from the directory database 34, but instead are read from the switch database 48 using the specific access method.

[0037] Figure 6 is a schematic flow diagram illustrating the operation of the directory service controller 60.

[0038] In step 110 a request is received from a DUA 38. The request can be, for example, a request to search for an attribute (e.g. a phone number) of a given distinguished name (DN), e.g.:

Search DN = < ANY DN > phone number

[0039] Here the distinguished name relates to an entry in the directory hierarchy, <ANY DN> relates to an appropriate key along the directory hierarchy chain and 'phone number' relates to the attribute being searched.

[0040] In step 112, the directory service controller 44 looks at the DACD for the appropriate domain in which the distinguished name is found to determine if an access method is identified for the attribute concerned.

[0041] If no access method is identified, then, in step 114, the directory controller accesses the requested access method from the directory database 14.

[0042] If an access method is found, then, in step 116, the directory controller retrieves the requested attribute using the access method concerned (for example by the issue of an appropriate GET message) and waiting for the response message.

[0043] The access methods could be defined statically or dynamically at each node in the directory 34.

[0044] Following step 114 or step 116, the accessed attribute is returned in step 118.

[0045] Although the present invention has been described specifically in the context of LDAP-based directory servers to permit the integration of non-X.500 data by employing ACLs to not only control access rights but also to define access methods, it will be appreciated that the invention can also be applied to other directory storage protocols. Indeed, the invention more generally provides the use of access control lists to define not only control access rights, but also to control access methods.

[0046] More generally, an embodiment of the invention can provide access to data in a predetermined environment (e.g. data stored in accordance with a different storage model from that on which the predetermined protocol is based, or a different physical location, or a different protocol) by configuring an attribute access method and using this method to retrieve the information from, for example a directory operable in the predetermined environment.

5 [0047] Also, although the storage of the ACL information has been described as being in the directory server, storage external to the directory server (e.g., in flat files) could also be employed. Further, the storage of the ACL information could be in the entry at the top of the subtree defined by the DACD, or indeed in all the entries in the DACD. Indeed, the location of the storage of the ACL information could be chosen according to a particular implementation or application.

10 [0048] Accordingly, it will be appreciated that although particular embodiments of the invention have been described, many modifications/additions and/or substitutions may be made within the scope of the present invention.

15 **Claims**

1. A computer-implemented directory access mechanism comprising:
 - i) a directory service operable to access a network directory under a predetermined protocol responding to an access request under said protocol for information available in a predetermined environment external to said directory; and
 - ii) said directory service using an access method for the environment to access said information.
2. The method of Claim 1, wherein said access method is retrieved from a domain definition for a domain of said directory.
- 25 3. The method of Claim 2, wherein said domain definition also comprises access control information.
4. The method of Claim 2 or Claim 3, wherein said directory is defined under X.500 and said access method is retrieved from a Directory Access Control Domain object.
- 30 5. The method of any one of Claims 2 to 4, wherein said domain definition comprises a pointer to an access method for said domain in said environment.
6. The method of Claim 5, wherein a said access control method is stored externally to said directory.
- 35 7. The method according to any one of Claims 2 to 6, wherein a said access control method is stored with a definition of a node in said directory.
8. The method of any preceding claim, wherein said protocol is the Lightweight Directory Access Protocol.
- 40 9. The method of any preceding claim, wherein said information is an attribute of an entry in said directory.
10. A directory access mechanism comprising:
 - 45 a directory service operable to access a network directory under a predetermined protocol; at least one identifier of an access method for access to information in a predetermined environment external to said directory; said directory service being configured to respond to an access request under said protocol to access said information in said environment using a said access method identifier.
 - 50 11. The mechanism of Claim 10, wherein said access method identifier(s) form part of a domain definition for a domain of said directory.
 12. The mechanism of Claim 11, wherein said domain definition also comprises access control information.
 - 55 13. The mechanism of Claim 11 or Claim 12, wherein said directory service is defined under X.500 and said access method identifier(s) form part of a Directory Access Control Domain.

14. The mechanism of any one of claims 11 to 13, wherein said domain definition comprises a pointer to an access method for said domain in said environment.
15. The mechanism of Claim 14, wherein a said access control method is stored externally to said directory.
16. The mechanism according to any one of Claims 11 to 15, wherein a said access control method is stored with a definition of a node in said directory.
17. The mechanism of any one of Claims 10 to 16, wherein said protocol is the Lightweight Directory Access Protocol.
18. The method of any one of Claims 10 to 17, wherein said information is an attribute of an entry in said directory.
19. A directory access mechanism comprising directory service means configured to be operable to access a network directory under a predetermined protocol and means for identifying at least one access method for access to information in a predetermined environment external to said directory, said directory service means being configured to respond to an access request under said protocol to access said information available in said environment using a said access method identifying means.
20. A computer implemented access control mechanism for an object-based directory, wherein said access control structure comprises:
 - control access rights for directory objects; and
 - access methods for attributes of said directory objects.
21. A computer program product on a carrier medium, said computer program product comprising:
 - a directory service configured to be operable to provide directory access under a predetermined protocol; and
 - at least one identifier of an access method for information in a predetermined environment, external to said directory,
 - 30 said directory service being configured to respond to an access request under said protocol to access said information available in said environment using a said access method identifier.
22. A directory server for a computer network, said directory server comprising:
 - 35 storage for a network services directory under a predetermined protocol and at least one identifier of an access method for information in a predetermined environment external to said directory; and
 - a processor for executing a directory service controller, said directory service being configured to respond to an access request under said protocol to access said information available in said environment using a said access method identifier.

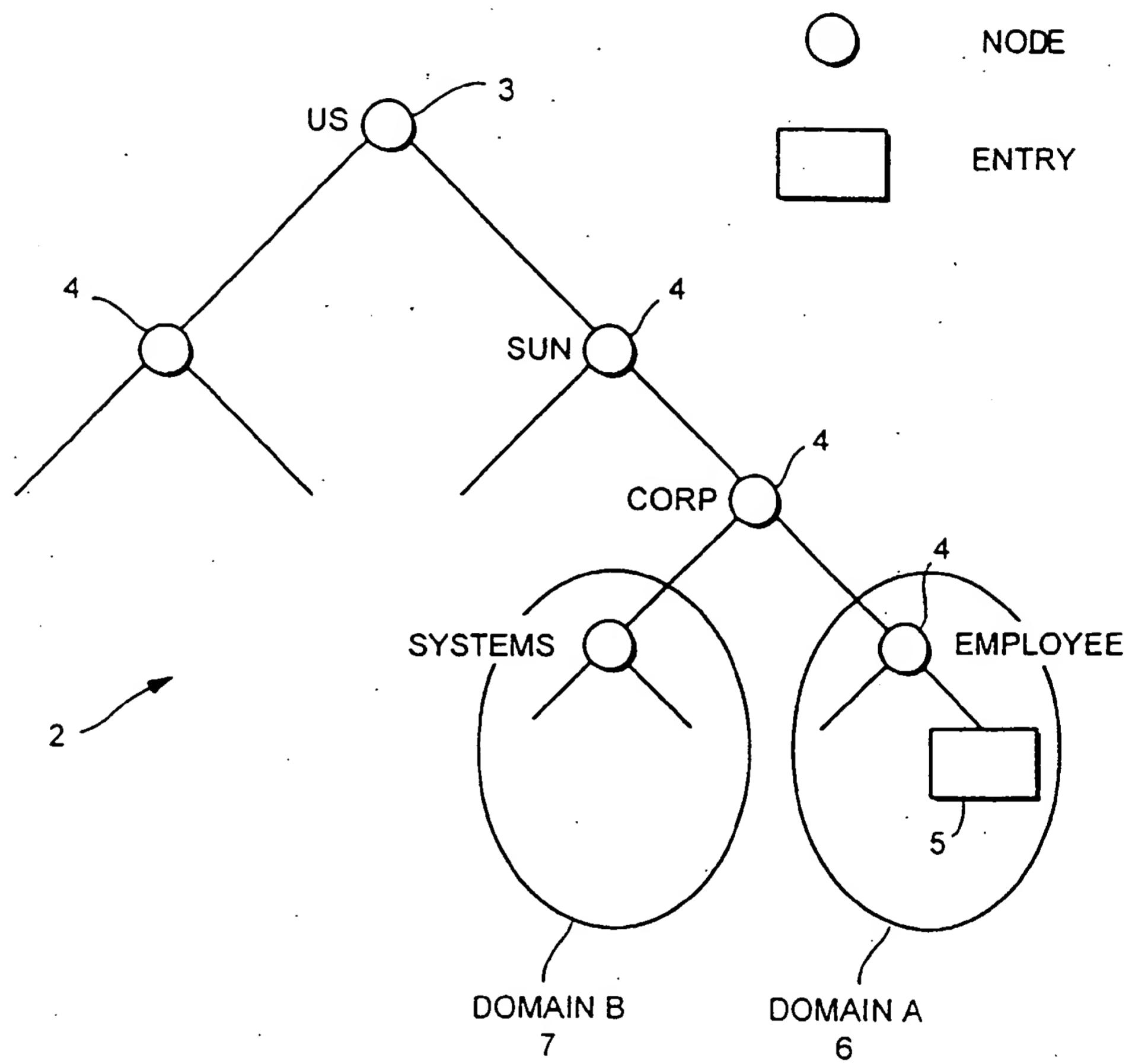


FIG.1.

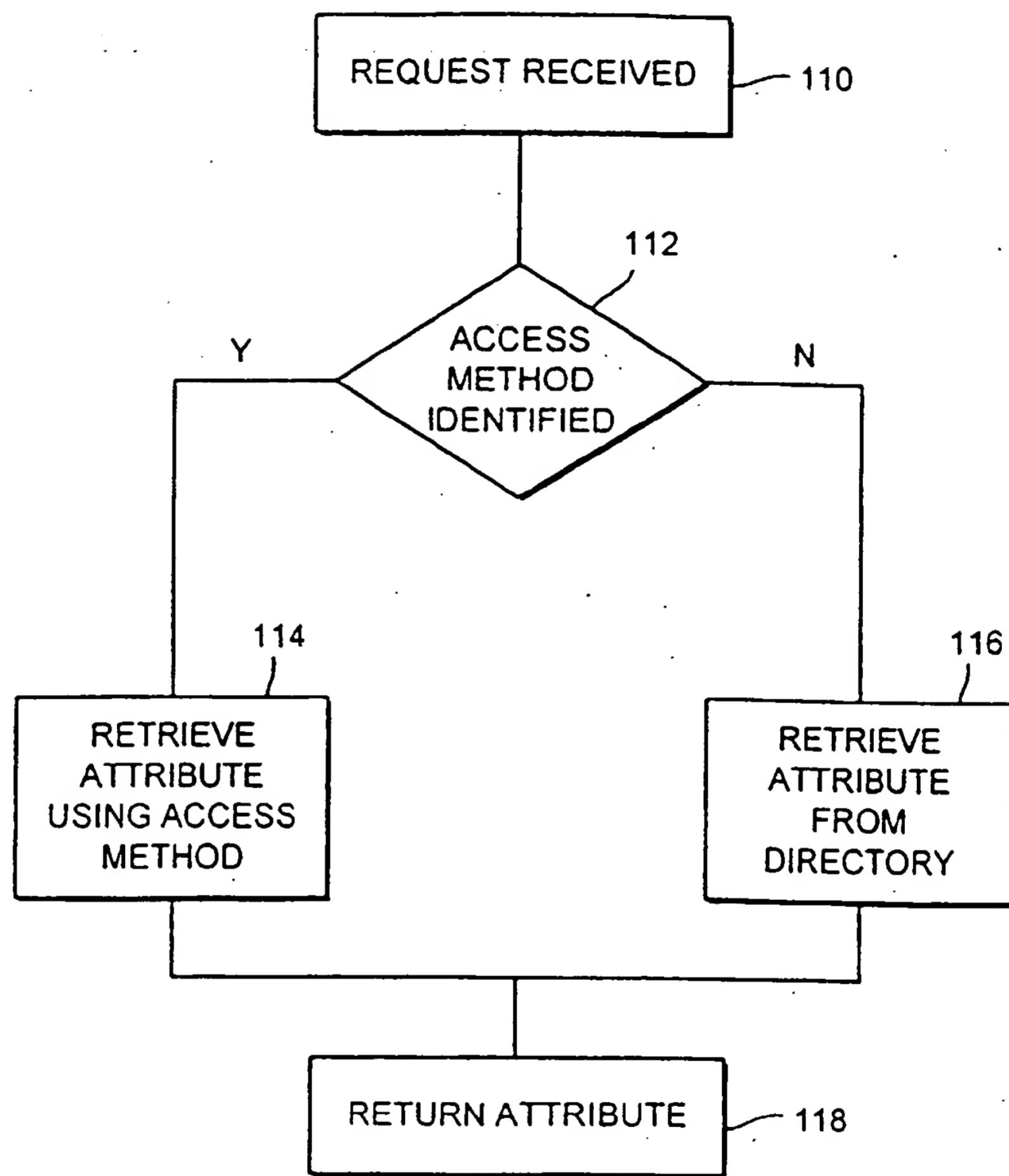


FIG.6.



DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	BRUNO L: "FINDING SOME DIRECTORY ASSISTANCE" DATA COMMUNICATIONS, vol. 27, no. 1, 1 January 1998 (1998-01-01), page 72, 74 XP000733527 ISSN: 0363-6399 * page 72, middle column, line 1 - right-hand column, line 20 * * page 74 *	1,8-10, 17-19, 21,22	H04L29/12
A	---	2-7, 11-16,20	
X	BRUNO L: "TIE IT ALL TOGETHER. DIRECTORIES HAVE GROWN IN COMPLEXITY AND SIZE - BUT THERE ARE WAYS TO CONTROL THE CHAOS" DATA COMMUNICATIONS, vol. 26, no. 3, 1 March 1997 (1997-03-01), pages 75-78, 80, 82/83, XP000659544 ISSN: 0363-6399 * figure 1; table 1 * * page 77, middle column, line 1 - page 78, left-hand column, line 12 *	1,8-10, 17-19, 21,22	
A	---	2-7, 11-16,20	H04L
A	ISO/IEC 9594-2: "Information technology - Open Systems Interconnection - The Directory: Models" ITU-T RECOMMENDATION X.501 (1993 E), 1993, pages 54-66, XP002114081 * page 57, line 1 - page 59, line 13 *	2-7, 11-16,20	

The present search report has been drawn up for all claims			
Place of search	Date of completion of the search	Examiner	
THE HAGUE	2 September 1999	Eraso Helguera, J	
CATEGORY OF CITED DOCUMENTS		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document	
X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document			



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 40 0380

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
P, X	<p>DATA CONNECTION LIMITED: "DC MetaLink Product Overview" PRODUCT DATASHEET, 'Online! August 1998 (1998-08), XP002114082 Retrieved from the Internet: <URL: http://www.datcon.co.uk/download/meta prov.ps.Z> 'retrieved on 1999-08-31! * the whole document *</p> <p>-----</p>	1,8-10, 17-19, 21,22	
			TECHNICAL FIELDS SEARCHED (Int.Cl.6)
	The present search report has been drawn up for all claims		
Place of search	Date of completion of the search		Examiner
THE HAGUE	2 September 1999		Eraso Helguera, J
CATEGORY OF CITED DOCUMENTS		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document	
X : particularly relevant; if taken alone Y : particularly relevant; if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document			

EP/FORM 1503/03.82 (IND/CO1)